WHAT IS CLAIMED IS:

1. A method for the generation of a pseudo-random permutation of an N-digit word in which:

- a generalized Feistel scheme is implemented,

wherein:

- the round functions of the generalized Feistel scheme implemented are functions (Fi) such that:

  - the input words of the round functions are produced by the conversion of digit words into binary words,
  - then a one-way function is applied to these binary words,
  - finally, the output in digits is a function of these binary words.

- a digit word to be enciphered is read in a memory,

- the generalized Feistel scheme used comprises at least T = 5 rounds.

.2. A method according to claim 1, wherein the one-way function on the binary words uses a standard pseudo-random cryptography function on binary words.

3. A method according to one of the claims 1 or 2 wherein the standard pseudo-random function on the binary words uses the SHA-1 function.

4. A method according to one of the claims 1 to 3 wherein the number of rounds T of the Feistel scheme is smaller than or equal to 30.

5. A method according to one of the claims 1 to 4, wherein the number of rounds T of the Feistel scheme is equal to 6.

6. A method according to one of the claims 1 to 5 wherein, during odd-valued rounds of the Feistel scheme, the round function works on a word with a length B, and during even-valued rounds of the Feistel scheme it works on words with a length of A digits, where A + B = N.

7 - A method according to claim 6, wherein A is equal to the integer part of N / 2 and B is equal to N - A.

8. A method according to one of the claims 1 to 7, wherein N is an integer contained in the interval [7, 30].

9. A method according to one of the claims 1 to 8, wherein N is an integer contained in the interval [10, 30].

10. A method according to one of the claims 1 to 8, wherein N is an

integer contained in the interval [13, 30].